Coronavirus Social Engineering Attacks: Issues and Recommendations

Ahmed Alzahrani
Faculty of Computing and Information Technology
King Abdulaziz University, Jeddah
Saudia Arabia

***Abstract*—During the current coronavirus pandemic, cybercriminals are exploiting people's anxieties to steal confidential information, distribute malicious software, perform ransomware attacks and use other social engineering attacks. The number of social engineering attacks is increasing day by day due to people's failure to recognize the attacks. Therefore, there is an urgent need for solutions to help people understand social engineering attacks and techniques. This paper helps individuals and industry by reviewing the most common coronavirus social engineering attacks and provides recommendations for responding to such an attack. The paper also discusses the psychology behind social engineering and introduces security awareness as a solution to reduce the risk of social engineering attacks.**

Keywords—Social engineering; coronavirus; COVID-19; phishing; vishing; smishing; scams; working remotely; cybersecurity; security awareness; human security behavior

I. Introduction

The entire world is suffering from the novel coronavirus or COVID-19, which has damaged the global economy and cybersecurity as well as causing death or damage to millions of people. While the world tries to deal with the coronavirus pandemic, cybercriminals are taking advantage of it to lure Internet users into becoming victims of social engineering attacks. For instance, cybercriminals are sending a huge amount of "phishing" attacks to trick users into clicking on malicious links or attachments so the criminals can steal sensitive data or lock users' devices and force them to pay a ransom to recover their data. Regardless of advanced security controls such as strong firewalls, cryptography methods, intrusion protection systems, and intrusion detection systems, social engineering still the biggest challenge to all organizations [1]. That's because of the human factor the attacker uses to conduct malicious activity when they cannot directly attack a system that has no technical vulnerabilities. Social engineering attacks are now considered as the most powerful security attacks [2]. The attacker uses psychological manipulation to convince users to violate security protocols. To perform a successful social engineering attack, the social engineer (attacker) needs to have a high level of skills, including the ability to fit the proper technique to manipulate a given victim. Relying on technical solutions to prevent such attacks is not practical, human users remain susceptible to manipulation by social engineers seeking to gain sensitive information or unauthorized access [3].

Social engineering attacks fall into four types: physical, technical, social, and socio-technical [3]. In general, there are two methods of social engineering attacks, human-based and computer-based. Human-based social engineering requires interaction with humans to gain the desired information. Impersonation is the most common approach for this type, via a phone call or text message (see Fig. 2), online, or even in person. Computer-based social engineering uses computer software to try to gain the required information. This attack includes sending scam emails asking the user to open an attachment to check the latest statistics about coronavirus or information about coronavirus safety measures (see Fig. 1). Cybercriminals can also create a fake website to trick users into downloading malware to steal users' credentials and online banking information.

The number of social engineering attacks during the coronavirus pandemic is increasing as cybercriminals exploit the situation for their selfish goals. This paper reviews the most common coronavirus social engineering issues and provides some recommendations for both individuals and industry. The paper is organized as follows: Section II provides a review of human security behavior. Section III describes the proper security awareness method to reduce the success of social engineering attacks. Section IV presents the study issues, followed by recommendations in Section V. Cybersecurity lessons from the coronavirus pandemic are discussed in Section VI and Section VII presents the study conclusions and future work.

II. Background

Social engineering attacks manipulate users to reveal sensitive information that the attacker may use against the target organizations. The Verizon [4] data breach investigation's recent report stated that 33% of actions used to attack organizations come through social engineering-based attacks. Therefore, there is a need to analyze the factors affecting human behavior to help security administrators plug gaps in information security.

A. Human Security Behavior

Most modern organizations depend on information systems. This requires them to manage associated risks such as social engineering attacks. The most challenging risks for an organization arguably center on information security. Many organizations tend to deploy technology-based solutions to mitigate these risks. These are necessary but often insufficient to address a range of potential threats. The human factor is an essential element of information security. According to the SANS institute [5], there are four categories of behavior that social engineers might use to manipulate human emotions to make a successful attack [5]. The first is a Careless Attack Vector, which helps the attacker exploit a failure to implement proper defensive countermeasures. A common example is password theft when the target has written it down on a piece of paper or a sticky note. Several research studies have tried to improve information-security practices, without significant success [6]. This is, therefore, a fresh examination of the challenges and obstacles related to the way people deal with the need for information security [7]. A number of real-life examples illustrate that complex and expensive security methods are not helpful if users compromise security measures by, for instance, neglecting password protection. Users regularly engage in intentional or non-intentional risk-taking behavior such as careless information handling, surfing on unsecured web-pages, thoughtless use of mobile devices or insecure data practices [8][9]. This type of risk-taking can open avenues through which malicious co-workers or external perpetrators can damage the organization. Second is a Comfort Zone Attack Vector which occurs when users feel comfortable in their environment, such as office, and do not realize the threat. A common technique is shoulder surfing, which means looking over the user's shoulder to get a username or password while the target types on their keyboard. Third: Helpful Attack Vector, which means users generally try to be helpful to everyone, including those they do not know. There are two kinds of direct attack types here.

- Direct Approach - Piggybacking: It’s called the “Big Box technique”: the attacker carries a big, heavy-looking box as they try to go through security doors [5]. A nearby employee sees this and opens the door to help the person with the box get in. The employee, with good intentions, gives the attacker access to the premises.
- Direct Approach - Impersonation: The attacker calls the organization’s IT help desk to gain information such as the target’s password. IT support has become aware of this kind of social engineering technique, but the risk should not be disregarded [5]. Another recent example is a scammer calling people and claiming to have a cure for coronavirus or offering a good deal of face masks. People who fall for the scammer provide their credit card information to complete the bogus transaction.

The “Fear Attack Vector” is classified as the most aggressive type of psychological attack [5]. The attacker makes use of the target’s fear, anxiety, stress, and pressure to get personal information or gain access to their accounts. For instance, the attacker pretends to be from a government department to trick the user to provide personally identifiable information.

The behavior of some users is probably influenced by the behavior of other users in their group or team [10]. The influencing factors involve both technical and non-technical factors related to protecting sensitive information [11]; both factors are equally important. Users can create, or make possible, many threats to the security of the organization, broadly divided into two classes [12]. The first kind of threat is intentional, involving malicious users who leak sensitive information. The second kind of risk is non-intentional actions, perhaps as a result of carelessness, resulting in leakage of information.

Consequently, information security is directly associated with the user’s security-related behavior. A good understanding of user security behavior can help reduce the success of social engineering attacks. For instance, “autonomy motivator” is a concept of self-determination theory, which focuses on human behavior and the extent to which behavior is self-motivated and self-determined [13]. Autonomy refers to "volition, having the experience of choice, endorsing one’s actions at the highest level of reflection” [13]. Since autonomy focusses on “the desire to protect an individual’s scope for action and decision-making” [14], users need to be supported in making the right decisions against a number of potential threats, known vulnerabilities of the infrastructure and past and ongoing cyber-attacks. This may help them to make the proper responses to real-world threats such as an e-mail link that might be a phishing attack. Alzahrani and Johnson [13] studied the autonomy motivator by investigating whether the user would fall victim to a phishing attack. The authors used the Decisions and Disruptions (D-D) cybersecurity game, which was developed by Professor Rashid and his team at the University of Bristol cybersecurity group [15]. The authors developed pre- and post-assessment tests on the autonomy motivator to find out whether there is a significant improvement in test scores after participants experience D-D gameplay. Overall results confirmed that the autonomy motivator is positively influenced by the game, which means players became more likely to make the right decision in response to social engineering techniques such as phishing or spear phishing. Users can gain or review valuable information from such awareness methods that may help them to increase their security awareness, which in turn may help them make the right decisions in the real world against social engineering attacks.

B. The Proper Security Awareness Method to Reduce the Success of Social Engineering Attacks

Many researchers identify the need for information security awareness to promote positive behaviors [16]. Since social engineering relies on the manipulation of human behavior, security experts consider raising awareness and training as the best way to combat social engineering attacks [3]. However, increasing awareness should be designed carefully and effectively by measuring its effect on users’ security behavior. Several efforts have been made to improve security awareness and develop methods for spreading awareness of cybersecurity among users. These methods can raise cybersecurity awareness regarding a wide range of social engineering threats. Important methods proposed in previous research include conventional, instructor-led, online, simulation-based, and game-based delivery methods. Each method has advantages and limitations. Organizations or government entities need to adopt the most suitable method to influence security awareness with respect to social engineering attacks.

Conventional delivery methods involve dissemination of cybersecurity awareness using paper and electronic resources. These methods use leaflets and posters for directing users' attention to specific and relevant subjects. This method has the advantage of sharing several messages at one time with the target audience [17]. However, it is challenging to ensure that users have gone through the newsletters and paper-based resources and understood the information that the documents seek to transmit.

Instructor-led delivery methods involve formal presentations, seminars, and classroom-based lectures facilitated by experts in the field to raise the cybersecurity awareness level of users. This method has its limitations. It is an expensive and static solution that usually results in a boring experience that is ineffective for the target audience [18]. The success of this method relies on the capability of the instructor to engage employees in the classroom. Limitations of this method can be addressed by sharing experiences and knowledge among users of an organization and ensuring their participation with interactive activities and group-work-based assignments.

Online delivery methods deliver cybersecurity awareness programs using e-mail broadcasts, online discussion, rich media, and interactive teaching applications. These methods are well suited for teaching over a distributed geographical area. Significant issues in using these methods involve the creation and implementation of an online cybersecurity awareness program as a result of the lack of fully developed plans for delivering it to the target audience and evaluating its effectiveness [18]. These methods require user self-motivation that often hinders the successful delivery of cybersecurity awareness.

Delivering cybersecurity awareness using educational video techniques plays a significant role. This method does not require a classroom trainer and addresses the limitations of conventional delivery methods for holding the trainee's attention for a long enough time to impart knowledge. Online video provides visual and audio learning for the target audience. Users can participate independently in the learning process at any particular time.

Simulation-based delivery methods have been attracting attention as a way to share cybersecurity information with users. [19]. This method could involve sharing simulated phishing emails to evaluate errors in employee response, or a phishing attack followed by training sessions on how to address such attacks.

Game-based delivery methods are another popular method that offer the most effective way to share cybersecurity awareness programs among users. These methods integrate graphics and play, or "gamification", into the training session to create a compelling experience for participants. Game-based delivery takes the players into a virtual space and simulates a real-world scenario to connect the players to circumstances and their consequences that may arise in the real world [20]. It offers the most effective way to share cybersecurity awareness programs among users. The primary advantage of the game-based delivery method for cybersecurity awareness is that it can challenge, motivate, and engage the target audience. Game-based delivery is a promising technique that can be combined with other approaches in a cybersecurity awareness training context to increase their effectiveness [21]. Game-based learning provides a safe environment in which players can practice their security behavior, and promotes self-learning across different learning styles [22]. Serious games also intrinsically motivate players to deal with game challenges by providing their own conclusions; as a result, they can improve their problem-solving skills [22]. Game-based learning offers an interactive method for training and educating the target audience on a specific subject or topic of social engineering. By playing the game, the target audience can enhance their skills during a fun and engaging experience. Game-based learning offers several advantages over more conventional means [20]. It can involve different case studies for motivating users in learning, according to their specific learning requirements.

Research on game-based learning suggests that it shows significant improvements in the level of players' understanding about setting strong passwords, identifying malware, the need for anti-malware programs, the nature of malware and phishing attacks, and using back-ups as a protective strategy. Game-based learning has achieved higher ratings in the heuristics evaluation process concerning awareness levels, usability, learning content, and fun and enjoyability features. Research found that participants prefer gamified environments over non-gamified environments [21]. Therefore, this may encourage organizations and government entities around the world, such as the computer emergency response team (CERT), to apply serious games to their awareness contexts to keep their users up to date about social engineering attacks and help reduce security breaches.

Also, it is recommended to use the Analytic Hierarchy Process (AHP) to support security decision-making to design effective security awareness programs [23]. AHP is a multiple-criteria decision-making tool used in several applications related to decision-making. One identifies the weights or the most important awareness focus area, to increase users' decision-making ability when they face real-world social engineering attacks. However, these weights may, in turn, be affected by local organizational and cultural factors. Users with the right security awareness method in place can potentially help prevent any kind of social engineering techniques. Table I shows a summary of seminal work in other cybersecurity serious games related to social engineering.

TABLE I. SUMMARY OF RECENT CYBER SECURITY SERIOUS GAMES

Game name	Game type	Goal	Results	Paper & Year
Untitled	Mobile Application.	To increase users' avoidance behavior through motivation to protect themselves against phishing threats.	The game had a positive effect on users' phishing avoidance behaviors.	[24] 2016
Untitled	Mobile Application	To increase participants' mobile threats awareness including phishing and cyber-attack.	The game increased the overall awareness of participants.	[25] 2017
Bird's Life	2D game via multiple platforms: PC, web, and mobile devices.	To improve phishing awareness among college students.	The game had a positive effect on players' understanding of phishing.	[26] 2018
Phishy	Web-based game portal	Phishy is a single-player game that trains enterprise users on phishing awareness.	Users showed a significant improvement in identifying phishing links.	[27] 2018
Pomega	2D Computer Game	To increase users' awareness across five topics: password, phishing, social network, mobile security, and physical security.	Users gained good knowledge about the five security awareness topics.	[28] 2019

III. ISSUES RELATED TO CORONAVIRUS SOCIAL ENGINEERING ATTACKS

A. *Coronavirus Malicious Attachments and Malware*

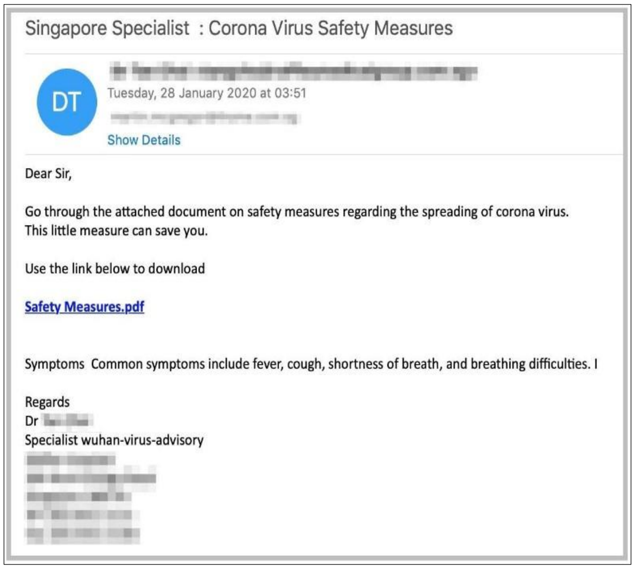
Malicious email attachments, posing as PDF files or Microsoft Word documents, are designed to attack the victims' computer once they open them. The main idea behind malicious software (malware) is to cause data loss without the target's consent. According to the World Health Organization (WHO) [29], cybercriminals are taking advantage of the coronavirus outbreaks by sending malicious attachments and links via email or social media applications such as WhatsApp. Hackers and cyber scammers claim to originate from WHO or any public health facilities to send malicious email attachments in the form of advice or information about the coronavirus pandemic. The Emotet is the most popular coronavirus-related malware [30] .It targets banking to obtain financial information. This Trojan malware program is spread through spam emails via attachment files, or malicious links to steal sensitive data.

Coronavirus map is another popular malware designed to trick users who want to keep track of how the virus is spreading around the world. This malware aims to steal users' personal information such as username, password, and credit card details. If the coronavirus continues to spread across globe, more applications will be developed to monitor it which, in turn, motivate cybercriminals to spread malware using the coronavirus theme.

B. *Coronavirus-Related Phishing, Vishing and Smishing*

Phishing is another type of social engineering attack that aims to steal users' sensitive personal information or online banking details, and which can result in identity theft and financial loss. Cybercriminals take advantage of users' anxiety about their health or finances by manipulating their emotions (fear) so they fall victim to social engineering attacks [31]. Cybercriminals are taking advantage of people's need for the latest coronavirus information by spreading phishing websites or using fake coronavirus payment websites to steal their money. For instance, The National Cyber Security Centre (NCSC) has removed more than 2,000 online scams related to coronavirus, including 471 fake online shops, 555 malware distribution sites, 200 phishing sites, and 832 advance-fee frauds [32]. Attackers also send phishing emails that appear to be from WHO or any authorized health organization to health care employees or users like an email with a PDF attachment that contains information about coronavirus safety measures shown in Fig. 1.

Spear phishing is advanced email phishing that targets well-researched victims such as high-level executives in an organization. The number of coronavirus-related spear-phishing attacks increased by 667% in March, 2020 [33]. According to Barracuda Networks [33] 11% of these attacks were blackmail attacks and conversation hijacking. Also, 77% of these attacks were scams, 22% were brand impersonation, and 1% were compromised business email. The goal of these attacks stealing users' personal information, distributing malware, and financial gain [33]. Attackers also use the Ransomware technique, which is a kind of malicious attack that blocks access to data or systems until a ransom is paid. Barracuda Networks noted that hackers have gained access to some users' information and threatened to infect it with coronavirus unless a ransom was paid.



Singapore Specialist : Corona Virus Safety Measures

[redacted]
Tuesday, 28 January 2020 at 03:51
[redacted]
Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Fig. 1. An Example of a Phishing Attack [31].

Hackers also use SmiShing, or Short Message Service (SMS) phishing attacks, to trick users into downloading any type of malicious code such as viruses or trojans to their mobile devices. The number of smishing attacks increased to 15,9688 in South Korea in Feb, 2020 [34]. The scammers used false information such as providing free face masks or alerts from fake delivery companies. Another common smishing method is using the UK government theme to collect emails, sensitive information, or banking information (see Fig. 2) [35]. The text message tricks people and looks like it is from "COVID" and "UKGOV" including a line to a phishing website.

Smishing is similar to phishing but the hackers use SMS instead of email [3]. Once the victim clicks the link, malicious code is installed on the device.

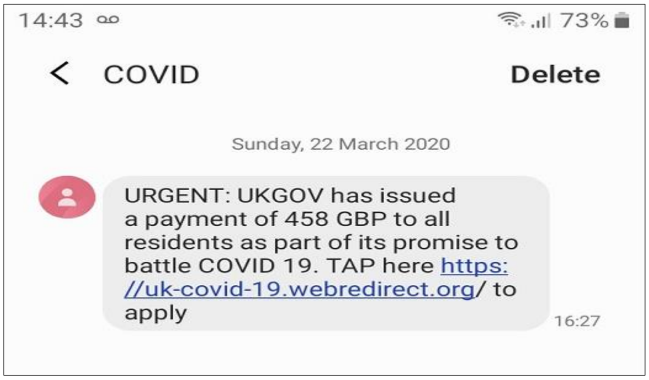
Vishing or voice phishing is a social engineering technique used to scam users via phone. For instance, the scammer may pretend a WHO employee who is collecting donations or asking for personal information [31]. These three are the most common scams during coronavirus crisis.

The attacks will continue until a cure is found. Meanwhile, security researchers keep investigating these attacks and help users avoid falling victim to any type of social engineering attack. Google blocks more than 100 million phishing emails every day, and 18 million coronavirus-related malware and phishing emails during April 2020 [36]. Similarly, WHO warned people about phishing that appeared to be from WHO and ask for sensitive information such as usernames or passwords, or invite the reader to click a malicious link or open a malicious attachment [29]. Additionally, the NCSC is investigated a huge number of phishing campaigns that had a bad effect on sectors such as transport, engineering, and defense [37]. The campaign includes the same phishing email theme (see Fig. 1) either by malicious links or PDF attachments.

C. Working Remotely due to the Coronavirus Pandemic

Due to the coronavirus pandemic, many organizations asked their employees to work from home and some staff may have no experience with working remotely. Therefore, this puts these organizations under pressure and raises more security challenges. As mentioned earlier, cybercriminals are exploiting coronavirus-related phishing via email to trick users online by sending suspicious emails contains malicious links or attachments. The scammers manipulate users' emotions by claiming to have a cure for coronavirus or offering financial support [38]. Such an attack may result in malicious code infection and data loss. Organizations need to support staff by providing awareness sessions to avoid such an attack.

A common attack related to working remotely is that hospitals' network gateway devices and Virtual Private Networks (VPN) vulnerabilities are targeted by ransomware campaigns called REvil or Sodinokibi, according to Microsoft [39]. Such an attack leads to stealing credentials and giving access to compromised networks to install ransomware or malware payloads [39]. Microsoft keeps advising organizations and people who use VPNs to work from home to apply security updates [40].



URGENT: UKGOV has issued a payment of 458 GBP to all residents as part of its promise to battle COVID 19. TAP here https://uk-covid-19.webredirect.org/ to apply

Fig. 2. An Example of Smishing Attack [35].

The following section provides recommendations and guidelines to mitigate the risk of coronavirus-related social engineering attacks among users. These recommendations can help individuals and industries prevent unauthorized access to their confidential information during this health crisis.

IV. Recommendations

A. Coronavirus Malicious Attachments and Malware

Cybercriminals are exploiting people's fear of the coronavirus to perform attacks across the globe. They lure the anxious through malicious attachments, fake websites, malicious links, or spam. To avoid falling victim to coronavirus-related malicious attachments and malware, users need to stay aware online and avoid opening email from an unknown address. However, if users' work requires dealing with customers by email, they need to check the attachments carefully, as any attachment might be malicious. Also, it is recommended to be aware of any email with "coronavirus" or "COVID-19" in its title; it should probably be ignored or deleted. People usually look for the latest information about coronavirus from WHO. Thus, it's worth reminding users that WHO never asks for personal information such as a password [29]. Also, WHO never asks to click on any link outside the WHO website and never asks for downloading email attachments that are not requested.

Moreover, users need to make sure to disable macros in their Microsoft Office applications to prevent macro malware [41]. Also, we recommend keeping the computer operating system and security software up to date, because hackers take advantage of security issues that manufacturers may have fixed with a patch, but before a user has installed the patch.

B. Coronavirus-Related Phishing, Vishing and Smishing

In the current coronavirus situation, cybercriminals use social engineering techniques to trick and convince users to fall victim to their attacks by clicking on a bad link or downloading email attachments (phishing), via phone scam calls (vishing) or by sending SMS containing malicious links to smart devices (smishing). This kind of attack can result in stealing sensitive information from the computer or smart devices, and distributing malware.

The common scam trick is that scammers claim to offer treatment for the coronavirus and use "Buy now, limited supply" to manipulate people's emotions [42]. The user needs to stay aware of any kind of request online or via phone that asks for personal information. Cybercriminals also use general greetings for phishing emails such as “Dear sir or madam”, without mentioning the receiver’s name (see Fig. 1) [42]. Another indication of a phishing email is including spelling and grammatical mistakes. User should delete such messages. Moreover, avoid visiting any website without checking its authenticity [43]. Websites which emails link to have a high risk of being malicious and including phishing links.

In general, NCSC listed some signs that may help people to avoid cyber scams [44].

- Authority: Scammers claim to be an official employee from an organization like a bank, healthcare sector, or government.
- Urgency: Scammers ask you to respond to their request immediately or within 24 hours.
- Emotion: Criminals manipulate people's emotions either by spreading fear or hope to trick them into cyber scams.
- Scarcity: Cybercriminals offer something with limited quantity such as medicine, face masks, or hand sanitizer. So people who fear missing a good deal may respond quickly.
- Current events: Scammers make use of current news stories or events such as tax refunds or donations for help to fight coronavirus to make their scam look real.

C. *Working Remotely*

Due to the coronavirus pandemic, most organizations across globe have their employees work from home, which may raise security challenges. NCSC provides some general recommendations to mitigate the risk of working remotely [45].

- The organization needs to provide its employees with clear guidelines on how to use their software, regardless of their experience level.
- Employees are already under stress due to the coronavirus pandemic, so organizations need to support them all the time not only by providing technical guides.
- Increase awareness among employees to avoid cybersecurity attacks such as coronavirus-themed emails, phishing, and scams.
- Educate employees on how to report a problem, especially security incidents.
- Encrypt data to protect it if devices are stolen, and keep the VPN fully patched.
- Disable removable media to prevent coronavirus malware.

Also, things users can do [46]:

- Configure Wi-Fi encryption, especially in older installations.
- The anti-virus software and operating system must be fully updated.
- Security tools such as privacy tools and add-ons for browsers must be up to date.
- Perform regular backups to protect against damaged or stolen data.
- Set up a screen lock for when a device must be left unattended.
- Turn on two-factor authentication for all accounts.

Furthermore, users need to stay vigilant by understanding the coronavirus-related phishing and malware in (Section V(A) and V(B) to support secure remote working.

V. Cybersecurity Lessons from the Coronavirus Pandemic

Here are brief recommendations based on lessons learned during the coronavirus pandemic. Organizations and government entities need to rethink planning for a worst-case scenario which will be useful in unexpected crises such as a pandemic. This could be done by studying the risks and finding ways to mitigate them. To build skilled and educated users, proper security awareness methods should be implemented, as discussed in Section III. This could be done by enterprises and CERT across the world. However, awareness is temporal in nature and it must be refreshed or renewed regularly to keep users motivated and updated about changing attack methods and trends. New technologies are emerging in addition to quick and challenging security risks to organizations or individuals who must be updated to remain aware. Finally, enhance the cybersecurity infrastructure such as firewalls and anti-malware software, and keep monitoring all activity within the network to detect any kind of compromises.

VI. Conclusion and Future Work

In conclusion, social engineering attacks can not be stopped by using only technology or security systems. Social engineers manipulate the users to access sensitive information. During the coronavirus pandemic, cybercriminals use psychological and analytical techniques to manipulate users. This study attempts to help individuals and industries by reviewing the most common coronavirus social engineering attacks, and provides recommendations to respond to such an attack. Cybercriminals make use of people's fear and anxiety about coronavirus by spreading malicious attachments purporting to provide covid-19 information and malware via email across the globe. Coronavirus-related phishing, vishing, and smishing are growing in frequency and intensity. Such attacks increase the chances of distributing malicious code, stealing sensitive information, and ransomware attacks. The paper discussed cybersecurity issues related to working remotely and provides recommendations to avoid security breaches.

Future work may analyze these coronavirus-related security issues to implement detection and countermeasure techniques to reduce the success of social engineering attacks. Similarly, attention should be paid to implementing proper social engineering awareness to reinforce good security behavior.

REFERENCES

[1] N. Pokrovskaia, S. S.- Management, T. And, and U. 2017, “Social engineering and digital technologies for the security of the social capital’development,” ieeexplore.ieee.org, pp. 16--18, 2017.

[2] A. M. Aroyo, F. Rea, G. Sandini, and A. Sciutti, “Trust and social engineering in human robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations or gamble?,” IEEE Robot. Autom. Lett., vol. 3, no. 4, pp. 3701–3708, 2018.

[3] A. Yasin, R. Fatima, L. Liu, A. Yasin, and J. Wang, “Contemplating social engineering studies and attack scenarios: A review study,” Secur. Priv., vol. 2, no. 4, Jul. 2019, doi: 10.1002/spy2.73.

[4] Verizon, “2019 Data Breach Investigations Report- Executive Summary,” 2019. Accessed: May 12, 2019. [Online]. Available: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

[5] C. Lively, “Psychological based social engineering,” SANS Inst., 2003.

[6] M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber security awareness campaigns: Why do they fail to change behaviour?,” arXiv Prepr. arXiv1901.02672, 2019.

[7] I. Kirlappos, S. Parkin, and M. S. Society, “Shadow security as a tool for the learning organization,” ACM SIGCAS Comput. Soc., vol. 45, pp. 29--37, 2015.

[8] M. Siponen and A. Vance, “Neutralization: new insights into the problem of employee information systems security policy violations,” MIS Q., pp. 487--502, 2010.

[9] J. Stanton, K. Stam, P. Mastrangelo, and J. Jolton, “Analysis of end user security behaviors,” Comput. Secur., vol. 24, no. 2, pp. 124--133, 2005.

[10] R. Cialdini and M. Trost, “Social influence: Social norms, conformity and compliance.,” McGraw-Hill, 1998.

[11] M. T. Siponen, “An analysis of the traditional IS security approaches: implications for research and practice,” Eur. J. Inf. Syst., vol. 14, no. 3, pp. 303–315, Sep. 2005, doi: 10.1057/palgrave.ejis.3000537.

[12] J. Leach, “Improving user security behaviour,” Comput. Secur., vol. 22, no. 8, pp. 685–692, 2003.

[13] A. Alzahrani and C. Johnson, “Autonomy Motivators, Serious Games, and Intention Toward ISP Compliance,” Int. J. Serious Games, vol. 6, no. 4, pp. 67–85, 2019.

[14] A. Alzahrani, C. Johnson, and S. Altamimi, “Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation,” in 2018 4th International Conference on Information Management (ICIM), May 2018, pp. 125–132, doi: 10.1109/INFOMAN.2018.8392822.

[15] R. Awais and B. Shreeve, “Decisions & Disruptions,” Lancaster University, CC-BY-NC, 2017. https://sites.google.com/view/decisions-disruptions/ (accessed Dec. 14, 2017).

[16] J. D’Arcy, A. Hovav, and D. Galletta, “User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach,” Inf. Syst., vol. 20, no. 1, pp. 79–98, 2009.

[17] M. Wilson, J. H.-N. S. Publication, and U. 2003, “Building an information technology security awareness and training program,” citadel-information.com, vol. 800, no. 50, pp. 1–39.

[18] J. Valentine, “Enhancing the employee security awareness model,” Elsevier, vol. 2006, no. 6, pp. 17--19, 2006.

[19] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” Commun. ACM, vol. 50, no. 10, pp. 94–100, 2007.

[20] S. Boyle, “An Introduction to Games based learning, sl: UCD Dublin,” 2011.

[21] I. Rieff, “Systematically Applying Gamification to Cyber Security Awareness Trainings,” 2018.

[22] A. Cook, R. Smith, L. Maglaras, and H. Janicke, “Using gamification to raise awareness of cyber threats to critical national infrastructure,” 2016.

[23] A. Alzahrani and C. Johnson, “AHP-based Security Decision Making: How Intention and Intrinsic Motivation Affect Policy Compliance,” Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 6, 2019, doi: 0.14569/IJACSA.2019.0100601.

[24] N. A. G. Arachchilage, S. Love, and K. Beznosov, “Phishing threat avoidance behaviour: An empirical investigation,” Comput. Human Behav., vol. 60, pp. 185–197, 2016, doi: 10.1016/j.chb.2016.02.065.

[25] N. Micallef and N. A. G. Arachchilage, “Involving users in the design of a serious game for security questions education,” arXiv Prepr. arXiv1710.03888, 2017.

[26] P. Weanquoi, J. Johnson, and J. Zhang, “Using a Game to Improve Phishing Awareness,” J. Cybersecurity Educ. Res. Pract., vol. 2018, no. 2, p. 2, 2019.

[27] G. CJ, S. Pandit, S. Vaddepalli, H. Tupsamudre, V. Banahatti, and S. Lodha, “Phishy-a serious game to train enterprise users on phishing awareness,” in Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts, 2018, pp. 169–181.

[28] V. Visoottiviseth, R. Sainont, T. Boonnak, and V. Thammakulkrajang, “POMEGA: Security game for building security awareness,” in Proceeding of 2018 7th ICT International Student Project Conference, ICT-ISPC 2018, 2018, pp. 1--6, doi: 10.1109/ICT-ISPC.2018.8523965.

[29] World Health Organization, “Beware of criminals pretending to be WHO,” 2020. https://www.who.int/about/communications/cyber-security.

[30] K. Okereafor and O. Adebola, “Tackling The Cybersecurity Impacts of the Coronavirus Outbreak as a Challenge to Internet Safety,” J. Homepage http//ijmr. net., vol. 8, no. 2, 2020.

[31] C. Conley, “Coronavirus Cyber Attacks - The Secret Threat | SANS Security Awareness,” 2020. https://www.sans.org/security-awareness-training/blog/coronavirus-cyber-attacks-secret-threat (accessed Apr. 24, 2020).

[32] National Cyber Security Centre, “Public urged to flag coronavirus related email scams as... - NCSC.GOV.UK,” 2020. https://www.ncsc.gov.uk/news/public-urged-to-flag-covid-19-threats-new-campaign (accessed Apr. 24, 2020).

[33] S. Magazine, “Coronavirus-Related Spear Phishing Attacks See 667% Increase in March 2020 | 2020-04-16 | Security Magazine,” 2020. https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020 (accessed Apr. 24, 2020).

[34] C. Mu-Hyun, “South Korea sees rise in smishing with coronavirus misinformation,” ZD Net, 2020. https://www.zdnet.com/article/south-korea-sees-rise-in-smishing-with-coronavirus-misinformation/#ftag=RSSbaffb68 (accessed Apr. 24, 2020).

[35] National Cyber Awareness System, “COVID-19 Exploited by Malicious Cyber Actors,” 2020. https://www.us-cert.gov/ncas/alerts/aa20-099a (accessed Apr. 24, 2020).

[36] N. Kumaran and S. Lugani, “Protecting against cyber threats during COVID-19 and beyond,” 2020. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond (accessed Apr. 24, 2020).

[37] National Cyber Security Centre, “Phishing campaign,” 2018. https://www.ncsc.gov.uk/news/phishing-campaign (accessed Apr. 24, 2020).

[38] National Cyber Security Centre, “NCSC issues guidance as home working increases in response,” 2020. https://www.ncsc.gov.uk/news/home-working-increases-in-response-to-covid-19 (accessed Apr. 25, 2020).

[39] Microsoft Security, “Microsoft works with healthcare organizations to protect from popular ransomware during COVID-19 crisis: Here’s what to do,” 2020. https://www.microsoft.com/security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-what-to-do/ (accessed Apr. 24, 2020).

[40] National Cyber Security Centre, “Weekly Threat Report 3rd April 2020 - NCSC.GOV.UK,” 2020. Accessed: Apr. 24, 2020. [Online]. Available: https://www.ncsc.gov.uk/report/weekly-threat-report-3rd-april-2020.

[41] Norton, “What Are Malicious Websites?,” 2020. https://us.norton.com/internetsecurity-malware-what-are-malicious-websites.html (accessed Apr. 25, 2020).

[42] S. Symanovich, “Coronavirus phishing emails: How to protect against COVID-19 scams,” Norton, 2020. https://us.norton.com/internet security-online-scams-coronavirus-phishing-scams.html (accessed Apr. 26, 2020).

[43] T. Ahmad, “Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity,” Available SSRN 3568830, 2020.

[44] National Cyber Security Centre, “Phishing attacks: dealing with suspicious emails and messages,” 2018. https://www.ncsc.gov.uk /guidance/suspicious-email-actions (accessed Apr. 26, 2020).

[45] National Cyber Security Centre, “Home working: preparing your organisation and staff,” 2020. https://www.ncsc.gov.uk/guidance/home-working (accessed Apr. 26, 2020).

[46] ENISA, “Top Tips for Cybersecurity when Working Remotely,” 2020. https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely (accessed Apr. 26, 2020